



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,884	03/08/2002	Jean-Sebastien Coron	032326-161	5848
21839	7590	06/15/2006	EXAMINER	
BUCHANAN INGERSOLL PC (INCLUDING BURNS, DOANE, SWECKER & MATHIS) POST OFFICE BOX 1404 ALEXANDRIA, VA 22313-1404			HENNING, MATTHEW T	
		ART UNIT	PAPER NUMBER	
			2131	

DATE MAILED: 06/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/913,884	CORON ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 29 March 2006.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 24-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 24-37 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 08 March 2002 is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    - a) All    b) Some \* c) None of:
      1. Certified copies of the priority documents have been received.
      2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
      3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: \_\_\_\_\_.

1 This action is in response to the communication filed on 3/29/2006.

## **DETAILED ACTION**

## *Response to Arguments*

4           Applicant's arguments with respect to claims 24-37 have been considered but are moot in  
5       view of the new ground(s) of rejection.

6 All rejections and objections not set forth below have been withdrawn.

7 Claims 1-23 have been cancelled and claims 24-37 have been examined.

## ***Claim Rejections - 35 USC § 112***

10 The following is a quotation of the second paragraph of 35 U.S.C. 112:

11 The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the  
12 subject matter which the applicant regards as his invention.

14       Claims 27 and 34 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite  
15      for failing to particularly point out and distinctly claim the subject matter which applicant  
16      regards as the invention. The claims recite that a plurality of successive rounds of DES comprise  
17      only the first three rounds and the last three rounds. However, DES has 16 rounds and therefore  
18      the combination of **only** the first three rounds and the last three rounds only is not a plurality of  
19      **successive** rounds. As such, the ordinary person would be unable to determine whether the  
20      scope of the claim. Therefore, the examiner will assume that the claim was meant to read that  
21      the plurality of successive rounds included the first three and last three rounds, as this can still fit  
22      the scope of successive rounds.

23

24

**1                   *Claim Rejections - 35 USC § 103***

2                 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all  
3                 obviousness rejections set forth in this Office action:

4                 (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in  
5                 section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are  
6                 such that the subject matter as a whole would have been obvious at the time the invention was made to a person  
7                 having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the  
8                 manner in which the invention was made.

9  
10               Claims 24-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et  
11               al. (US Patent Number 6,278,783) hereinafter referred to as Kocher, and further in view of Ohki  
12               et al. (US Patent Number 6,615,354) hereinafter referred to as Ohki.

13               Regarding claim 24, Kocher disclosed a countermeasure method in an electronic  
14               component that implements the DES cryptographic algorithm in which multiple rounds of  
15               calculation are performed on input data (See Kocher Abstract), wherein each round of  
16               calculation includes at least the following operations: a first permutation of data (See Kocher  
17               Col. 10 Lines 55-60); manipulation of the permuted data by a secret key (See Kocher Col. 10  
18               Line 61 – Col. 11 Line 5); a table look-up operation based on the manipulated data (See Kocher  
19               Col. 11 Lines 6-7); and a second permutation of data (See Kocher Col. 11 Lines 7-11), but  
20               Kocher failed to disclose wherein, for a plurality of successive rounds of said algorithm, at least  
21               one of said first and second permutations of data comprises the following steps: selecting a first  
22               random value having the same size as the data being permuted, performing an exclusive-or  
23               operation between the data being permuted and the first random value to generate a second  
24               random value, executing said permutation operation on each of the first and second random  
25               values, to generate respective first and second random results, and performing an exclusive-or  
26               operation between said first and second random results to produce a final permuted result.

Art Unit: 2131

1            Ohki teaches that in order to protect against current analysis in a smartcard, processes,  
2 including permutation, should be performed using disturbance data (See Ohki Col. 3 Paragraph  
3 2). Ohki further describes that the permutation operations should be altered by selecting a first  
4 random value having the same size as the data being permuted, performing an exclusive-or  
5 operation between the data being permuted and the first random value to generate a second  
6 random value, executing said permutation operation on each of the first and second random  
7 values, to generate respective first and second random results, and performing an exclusive-or  
8 operation between said first and second random results to produce a final permuted result (See  
9 Ohki Col. 3 Lines 32-63).

10          It would have been obvious to the ordinary person skilled in the art at the time of  
11 invention to employ the teachings of Ohki in the DES system of Kocher by performing the  
12 permutation processing according to the disturbance data method of Ohki. This would have been  
13 obvious because the ordinary person skilled in the art would have been motivated to protect the  
14 permutation processing from current analysis.

15          Regarding claim 31, Kocher disclosed an electronic component that implements the DES  
16 cryptographic algorithm in which multiple rounds of calculation are performed on input data,  
17 said electronic component including a microprocessor that executes the following operations  
18 during each round of calculation (See Kocher Abstract): a first permutation of data (See Kocher  
19 Col. 10 Lines 55-60); manipulation of the permuted data by a secret key (See Kocher Col. 10  
20 Line 61 – Col. 11 Line 5); a table look-up operation based on the manipulated data (See Kocher  
21 Col. 11 Lines 6-7); and a second permutation of data (See Kocher Col. 11 Lines 7-11), but  
22 Kocher failed to disclose wherein, for a plurality of successive rounds of said algorithm, at least

Art Unit: 2131

1 one of said first and second permutations of data comprises the following steps: selecting a first  
2 random value having the same size as the data being permuted, performing an exclusive-or  
3 operation between the data being permuted and the first random value to generate a second  
4 random value, executing said permutation operation on each of the first and second random  
5 values, to generate respective first and second random results, and performing an exclusive-or  
6 operation between said first and second random results to produce a final permuted result.

7 Ohki teaches that in order to protect against current analysis in a smartcard, processes,  
8 including permutation, should be performed using disturbance data (See Ohki Col. 3 Paragraph  
9 2). Ohki further describes that the permutation operations should be altered by selecting a first  
10 random value having the same size as the data being permuted, performing an exclusive-or  
11 operation between the data being permuted and the first random value to generate a second  
12 random value, executing said permutation operation on each of the first and second random  
13 values, to generate respective first and second random results, and performing an exclusive-or  
14 operation between said first and second random results to produce a final permuted result (See  
15 Ohki Col. 3 Lines 32-63).

16 It would have been obvious to the ordinary person skilled in the art at the time of  
17 invention to employ the teachings of Ohki in the DES system of Kocher by performing the  
18 permutation processing according to the disturbance data method of Ohki. This would have been  
19 obvious because the ordinary person skilled in the art would have been motivated to protect the  
20 permutation processing from current analysis.

Art Unit: 2131

1       Regarding claims 25 and 32, Kocher and Ohki disclosed that both of said first and second  
2   permutation operations in each of said plurality of successive rounds (See the rejection of claims  
3   24 and 31 above).

4       Regarding claims 26 and 33, Kocher and Ohki disclosed that the first and second  
5   permutation operations utilize different respective first random values (See Ohki Col. 13 Line 66  
6   – Col. 14 Line 3).

7       Regarding claims 27 and 34, Kocher and Ohki disclosed that said plurality of successive  
8   rounds comprise only the first three and the last three rounds of said algorithm (See Ohki Col. 13  
9   Line 66 – Col. 14 Line 3).

10       Regarding claims 28 and 35, Kocher and Ohki disclosed that the manipulation operation  
11   performed during said plurality of successive rounds comprises the following steps: performing  
12   an exclusive-or operation between said secret key and a third random value having the same size  
13   as said key, to generate a fourth random value; performing bit-by-bit operations on each of said  
14   third and fourth random values to produce a pair of intermediate keys; manipulating the result of  
15   said first permutation operation with one of said intermediate keys to produce an intermediate  
16   result, and manipulating said intermediate result with the other of said intermediate keys to  
17   produce an output data item (See Kocher Col. 10 Lines 16-24 and the rejections of claims 24 and  
18   31 above).

19       Regarding claims 29 and 36, Kocher and Ohki disclosed that said manipulating steps  
20   comprise exclusive-or operations (See Ohki Col. 3 Lines 32-36).

Art Unit: 2131

Regarding claims 30 and 37, Kocher and Ohki disclosed that said bit-by-bit operations comprise a key permutation operation, a shift operation and a compression permutation operation (See Kocher Col. 10 Lines 16-24).

### *Conclusion*

Claims 1-23 have been cancelled and claims 24-37 have been rejected.

6 Applicant's amendment necessitated the new ground(s) of rejection presented in this  
7 Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

8 Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE (3) weeks from the mailing date of this action.

9           A shortened statutory period for reply to this final action is set to expire THREE  
10          MONTHS from the mailing date of this action. In the event a first reply is filed within TWO  
11          MONTHS of the mailing date of this final action and the advisory action is not mailed until after  
12          the end of the THREE-MONTH shortened statutory period, then the shortened statutory period  
13          will expire on the date the advisory action is mailed, and any extension fee pursuant to 37  
14          CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,  
15          however, will the statutory period for reply expire later than SIX MONTHS from the date of this  
16          final action.

17 Any inquiry concerning this communication or earlier communications from the  
18 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.  
19 The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

1         Information regarding the status of an application may be obtained from the Patent  
2         Application Information Retrieval (PAIR) system. Status information for published applications  
3         may be obtained from either Private PAIR or Public PAIR. Status information for unpublished  
4         applications is available through Private PAIR only. For more information about the PAIR  
5         system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR  
6         system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would  
7         like assistance from a USPTO Customer Service Representative or access to the automated  
8         information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

9

10

11

12

13

CHRISTOPHER REVAK  
PRIMARY EXAMINER



14         Matthew Henning  
15         Assistant Examiner  
16         Art Unit 2131  
17         6/9/2006

18